Elementare Zahlentheorie (VU) – Sommersemester 2022

Nachklausur – 6.10.2022

- Lösen Sie jede Aufgabe auf einem separaten Blatt (die erste Aufgabe können Sie am Deckblatt lösen).
- Schreiben Sie auf jedes Blatt Ihren Namen und Ihren Gruppenleiter!

Name: **Matrikelnr.:**

Gruppe: ☐ **1 (Smertnig, früh)** ☐ **2 (Fripertinger)** ☐ **3 (Smertnig, spät)** ☐ **4 (Fadinger)**

Pro Aufgabe sind **2 Punkte** zu erreichen. Viel Erfolg!

Aufgabe 1 (Kurzfragen) (a) (**1 P.**) Seien $n \in \mathbb{N}$, $a_1, \dots, a_n \in \mathbb{Z}$ und $d \in \mathbb{N}_0$.
Es ist $d = \mathrm{ggT}(a_1, \dots, a_n)$ genau dann, wenn gilt $d \mid a_i$ für alle $i \in [1, n]$ ...

☐ ..., und ist $d' \in \mathbb{N}_0$ mit $d' \mid a_i$ für alle $i \in [1, n]$, so folgt $d' \mid d$.
☐ ..., und ist $d' \in \mathbb{N}_0$ mit $d' \mid a_i$ für alle $i \in [1, n]$, so folgt $d \mid d'$.
☐ ..., und es gibt $x_1, \dots, x_n \in \mathbb{Z}$ mit $d = a_1x_1 + \cdots + a_nx_n$.
☐ ..., und es gibt ein $d' \in \mathbb{N}_0$ mit $d' \mid a_i$ für alle $i \in [1, n]$ und $d' \mid d$.

(*Kreuzen Sie die wahren Aussagen an; ohne Beweis*)

(b) (**1 P.**) Geben Sie ein vollständigen Restsystem modulo 7 an, welches nur aus *geraden* Zahlen besteht.

$$\{ \qquad\qquad\qquad\qquad\qquad\qquad \}.$$

Aufgabe 2 (2 P.)
Bestimmen Sie die letzten beiden Dezimalziffern von 7^{492} und von 7^{494} (d.h. Einerziffer und Zehnerziffer).

Aufgabe 3 (2 P.)
Seien m, $m' \in \mathbb{N}$ und seien weiters a, a', b, b', $x \in \mathbb{Z}$, so dass gilt

$$ax \equiv b \mod m \quad \text{und} \quad a'x \equiv b' \mod m'.$$

Zeigen Sie: Es gilt $ab' \equiv a'b \mod d$, wobei $d := \mathrm{ggT}(m, m')$.

Aufgabe 4 (2 P.)
Formulieren (**1 P.**) und beweisen (**1 P.**) Sie **einen** der folgenden beiden Sätze:

- Charakterisierung der Körper unter den Restklassenringen $\mathbb{Z}/m\mathbb{Z}$ ($m \geq 1$).
- Chinesischer Restsatz (für Kongruenzen).